control list relates user identification to available documents. Documents to which a user does not have access will not be listed or returned to the client who does not have control of access. The search will only display documents which correspond to the user's access level.

In contrast, the Schloss patent discloses a system and method which allows a user to control access to data located on a content server. An advisory server rates the content of data from a content server and sends a classification rating back to a client. The client then elects whether or not to display the content based upon the classification rating and the client's selected preferences.

The Examiner contends that it would have been obvious in view of Schloss for the present invention to do the screening at the web server, rather than at the client of Schloss. The Applicant asserts, however, that conducting the process at the server markedly changes and improves upon the claimed operation of the Schloss system and method. The Office action states in paragraph 6 that, "...it was known in the art that computing an operation at the server where it is requested and returning the result is faster and more efficient that (sic) providing a response which must then be computed by the client." The Applicant respectfully disagrees with this statement as it is applied to the present invention. Client-Server architecture was specifically designed to distribute the processing load among the clients and servers, thereby increasing network efficiency. Computing an operation at the server is not necessarily the fastest and most efficient route. This is evidenced by the Schloss patent which clearly specifies the desire to control content delivery at the client. Even if the Examiner's contention were correct, the two patents describe and claim different methods of access control which run counter to one another. Schloss allows the user to control access. Applicant does not.

The present invention utilizes server-based architecture to determine access for several reasons. First, much greater security and control is available at the server. There is much less susceptibility to bypassing a server-based control than a client-based control. A secure and monitored web server determines validity in the present invention, whereas an unsecure client terminal controls access in Schloss. An important, and not insubstantial, difference between the two methods is that the client of Schloss optionally selects the advisory preferences, while the server of the present invention dictates what content will be displayed to a particular client. The Schloss client can deselect particular information based on personal preferences, that would otherwise be normally downloadable from the server. The client of the present method would not even be aware of content that is screened form such client.

<u>Schloss specifically claims a client-side method</u>, wherein the method inhibits the loading of certain content based on a rating by and advisory server. When basing filtering information on individual advisory preferences, a client based method is more efficient, as advisory preferences can change based on user needs. For some instances it would be desirable to block certain content, while in another instance the user might need access to that content. For example, under the Schloss patent a user could select not to receive violent content. Yet, later in the day the user could elect to ignore the advice and view violent content when it pertained to war or military action. Needs change, and the advisory services disclosed by Schloss allow the client to change their advisory options whenever the client so chooses. In this situation, it would not be efficient to have the access control based at the server, as the client would not have any control over content delivery. The Schloss client need only change settings

to change the content delivery, while the servers of the present invention have exclusive control over information delivery.

The advisory server of Schloss is very different from the access control list of the present invention, and it would not have been obvious to create the present invention in view of Schloss. In Schloss, it is up to the client to determine what direction to take based upon information from the advisory server. Content will be blocked if the user so desires, but such control remains within the province of the user. Whereas, the present invention only displays information to the client which is approved by the access control list. Therefore, a much more secure environment for information distribution is created by the present invention.

Another important difference between the present invention and Schloss is the way in which content is blocked from the client. In the present invention, prohibited URLs and related content are not displayed to the client. The client is never aware of the blocked material, as the server filters the material before delivering it to the user. This increases security because the user does not know that certain material has been blocked. In contrast, Schloss displays all of the URLs and only blocks a specific page once it is requested and then denied by the advisory server. Therefore, a user must actually request material before it is blocked by the advisory server. As a result, the user is aware of content blocking, which may lead to an increased likelihood of attempts to compromise the advisory system. (See Abstract, Col. 7 lines 1-25, and Col. 8 lines 40-54 of the Schloss patent). The issue is who controls access.

An obviousness rejection cannot stand where the teachings of the reference run counter to the teachings of the Applicant. Schloss teaches that the user can control access. Applicant teaches and claims that users are screened from access by web servers. The obviousness rejection based on Schloss is believed to be traversed.

The other reference cited in the Office action, a patent to Kirsch (U.S. Patent No. 5,751,956), does not relate to the problem of controlling the transmission of documents from a web server to a client. This patent discloses a method and apparatus for redirection of server external hyper-link references. Kirsch claims a method to redirect URL information to a second server system for accounting and other services. This allows URL locations to be moved and have the old URL automatically refer the user to the new URL. The validation that is performed under Kirsch relates to assessing the validity of the referring webpage and other information. Client validation is performed, but only to the extent of providing access to the server itself. Access and retrieval of particular information contained on the server is not anticipated by Kirsch. (See Figs. 3 and 4, and Col. 9 line 51 to Col. 10 line 23 of the Kirsch patent).

In view of the remarks made herein, the Applicant requests reconsideration of the claims. A Notice of Allowance is earnestly solicited.

CERTIFICATE OF MAILING

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Asst. Commissioner for Patents, Washington, D.C. 20231

Signed: Sally Azevedo
Typed Name: Sally Azevedo

Date: November 12, 1999

Respectfully submitted,

Thomas Schneck

Thomas Schneck
Reg. No. 24,518

P.O. Box 2-E
San Jose, CA 95109-0005
(408) 297-9733